IN THE CLAIMS:

A status of all the claims of the present Application is presented below:

1. (Original) A computer security system, comprising:

a self-managed device having an authentication system for controlling access to the self-managed device by a user; and

a security module adapted to authenticate an identity of the user and, in response to user authentication, automatically generate, transparently to the user, device credential data verifiable by the authentication system to enable user access to the self-managed device.

2. (Original) The system of Claim 1, wherein the security module is adapted to randomly generate the device credential data.

3. (Original) The system of Claim 1, wherein the security module is adapted to automatically transmit, transparently to the user, the device credential data to the self-managed device.

4. (Original) The system of Claim 1, wherein the security module is adapted to receive a request from a networked administration client to activate the authentication system of the self-managed device.

5. (Original) The system of Claim 1, wherein the security module is disposed within a basic input/output system (BIOS).

6. (Original) The system of Claim 1, wherein the security module is adapted to access relational data correlating the user to the device credential data for the self-managed device.

7. (Original) The system of Claim 1, further comprising an activation/deactivation module accessible by an administration client to activate the authentication system of the self-managed device.

8. (Original) The system of Claim 1, further comprising an activation/deactivation module accessible by an administration client to deactivate the authentication system of the self-managed device.

9. (Original) The system of Claim 1, wherein the security module is adapted to receive a request from a networked administration client to deactivate the authentication system of the self-managed device.

10. (Original) The system of Claim 1, wherein the security module is adapted to perform a registration operation to register the self-managed device.

11. (Original) A computer security system, comprising:

means for controlling user access to a self-managed device; and

means for authenticating an identity of the user and, in response to user authentication, automatically generating, transparently to the user, device credential data verifiable by the controlling means to enable user access to the self-managed device.

12. (Original) The system of Claim 11, further comprising means for automatically transmitting the device credential data, transparently to the user, to the self-managed device for verification by the controlling means.

13. (Original) The system of Claim 11, further comprising means for correlating the device credential data with the user.

14. (Original) The system of Claim 11, further comprising means for receiving a request from a networked administration client to activate the controlling means.

15. (Original) The system of Claim 11, further comprising means for randomly generating the device credential data.

16. (Original) A computer security method, comprising:

authenticating an identity of a user; and

automatically generating transparently to the user, in response to user authentication, device credential data verifiable by an authentication system of a self-managed device to enable user access to the self-managed device.

17. (Original) The method of Claim 16, further comprising automatically transmitting, transparently to the user, the device credential data to the self-managed device.

18. (Original) The method of Claim 16, further comprising randomly generating the device credential data.

19. (Original) The method of Claim 16, further comprising receiving a request from a networked administration client to activate the authentication system of the self-managed device.

20. (Original) The method of Claim 16, further comprising receiving a request from a networked administration client to deactivate the authentication system of the self-managed device.

21. The method of Claim 16, further comprising initiating an activation/deactivation module to enable activation of the authentication system.

22. (Original) The method of Claim 16, further comprising accessing relational data correlating the device credential data with the user.

23. (Original) The method of Claim 16, further comprising storing the device credential data at the self-managed device.

24. (Original) The method of Claim 16, further comprising performing a registration operation to register the self-managed device to the user.

25. (Original) A computer security system, comprising:

a security module executable by a processor, the security module adapted to access credential data to verify an identity of a user; and

an activation/deactivation module accessible via a networked administration client, the activation/deactivation module adapted to interface with the security module in response to a request by the administration client to activate, transparently to the user, an authentication system of a self-managed device to control user access to the self-managed device.

26. (Original) The system of Claim 25, wherein the security module is adapted to automatically generate, transparently to the user, a device credential for verification by the authentication system.

27. (Original) The system of Claim 25, wherein the security module is adapted to randomly generate, transparently to the user, a device credential for verification by the authentication system.

28. (Original) The system of Claim 25, wherein the security module is adapted to transmit, transparently to the user, a device credential to the device for verification by the authentication system.

29. (Original) The system of Claim 25, wherein the activation/deactivation module is adapted to display to the user registered self-managed devices available for authentication system deactivation.

30. (Original) The system of Claim 25, wherein the security module is adapted to correlate a device credential for verification by the authentication system with the user.

31. (Original) A computer network security system, comprising:

a security module adapted to automatically generate, transparently to a user, device credential data verifiable by an authentication system of a self-managed device to enable user access to the self-managed device; and

an activation/deactivation module adapted to receive a request from the user to automatically activate the authentication system of the self-managed device.

32. (Original) The system of Claim 31, wherein the security module is adapted to automatically transmit, transparently to the user, the device credential data to the authentication system.

33. (Original) The system of Claim 31, wherein the self-managed device is adapted to store the device credential data received from the security module.

34. (Previously presented) The system of Claim 31, wherein the security module is disposed within a basic input/output system (BIOS).

35. (Original) The system of Claim 31, wherein the activation/deactivation module is adapted to receive a request from a networked administration client to activate the authentication system.

36. (Original) The system of Claim 31, wherein the security module is adapted to randomly generate the device credential.

37. (Currently amended) A computer security method, comprising:

authenticating an identity of a user; and

if successfully authenticated, generating and transmitting, transparently to the user, device credential data to a self-managed device for authentication by the self-managed device to enable the user to access the self-managed device.

38. (Original) The method of Claim 37, further comprising correlating the identity of the user to the device credential data.

39. (Original) The method of Claim 37, further comprising performing a registration operation to register the self-managed device.

40. (Original) The method of Claim 37, further comprising encrypting the device credential data.

41. (Original) The method of Claim 37, wherein transmitting comprises transmitting, transparently to the user, encrypted device credential data to the self-managed device for decryption by the self-managed device to authenticate access to the self-managed device.

42. (New) An electronic device, comprising:

a self-managed device disposed within the electronic device and configured to manage user access to the self-managed device; and

a security module disposed within a basic input/output system (BIOS) of the electronic device and, in response to user authentication, configured to automatically generate, transparently to the user, device credential data verifiable by an authentication system of the self-managed device.

43. (New) The electronic device of Claim 42, wherein the security module is configured to randomly generate the device credential data.

44. (New) The electronic device of Claim 42, wherein the security module is configured to receive a request from a networked administration client to activate the authentication system of the self-managed device.

45. (New) The electronic device of Claim 42, further comprising an activation/deactivation module accessible by an administration client to activate the authentication system of the self-managed device.

46. (New) The electronic device of Claim 42, wherein the security module is configured to receive a request from a network administration client to deactivate the authentication system of the self-managed device.